Cisco IOS XE ソフトウェアの Web UI で発見されたコマンド インジェクションの脆弱性

High

アドバイザリーID : cisco-sa-20190925-webui-cmd-injection
初公開日 : 2019-09-25 16:00
最終更新日 : 2019-10-14 18:25
バージョン 1.2 : Final
CVSSスコア : 7.6
回避策 : No workarounds available
Cisco バグ ID : CSCvo61821 CSCvp95724 CSCvp78858

CVE-2019-12650
CVE-2019-12651

日本語による情報は、英語による原文の非公式な翻訳であり、英語原文との間で内容の齟齬がある場合には、英語原文が優先します。

概要

Cisco IOS XE ソフトウェアの Web ベースのユーザ インターフェイス (Web UI) で複数の脆弱性が確認されました。認証されたリモートの攻撃者が、昇格された権限を使用して、標的デバイスでコマンドを実行する危険性があります。

これらの脆弱性の詳細については本アドバイザリの「詳細情報」セクションを参照してください。

シスコはこれらの脆弱性に対処するソフトウェア アップデートを提供しています。 これらの脆弱性に対処する回避策はありません。

このアドバイザリは、次のリンクより確認できます。
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190925-webui-cmd-injection

このアドバイザリは、2019 年 9 月 25 日に公開された Cisco IOS および IOS XE ソフトウェア リリースのセキュリティ アドバイザリ資料の一部です。この資料には、13 件の脆弱性に関する 12 件のシスコ セキュリティ アドバイザリが記載されています。 これらのアドバイザリとリンクの一覧については、以下を参照してください。シスコのイベント対応： Cisco IOS および IOS XE ソフトウェアに関するセキュリティ アドバイザリ公開資料 (半年刊、2019 年 9 月)

該当製品

脆弱性のある製品

この脆弱性の影響を受けるのは、シスコ デバイスで脆弱性のある IOS XE ソフトウェア リリースを稼動しており、HTTP サーバ機能が有効になっている場合です。

HTTP サーバ機能のデフォルトの状態は、バージョンによって異なります。

脆弱性が存在する Cisco IOS XE ソフトウェア リリースについては、このアドバイザリの「修正済みソフトウェア」セクションを参照してください。

HTTP サーバ設定の確認

HTTP サーバ機能がデバイスで有効かどうかを確認するには、管理者がデバイスにログインして CLI で **show running-config | include ip http server |secure-server** コマンドを使用し、グローバル コンフィギュレーションに **ip http server** コマンドまたは **ip http secure-server** コマンドが含まれるかどうかを確認します。 どちらかのコマンドが含まれ、設定されている場合は、HTTP サーバ機能が有効です。

次に、 IPv4 ヘルパー アドレスが設定されたデバイス上の **show running-config | include ip http server |secure-server** コマンドの出力を示します。このデバイスでは HTTP サーバ機能が有効になっています。

```
Router# show running-config | include ip http server|secure-server
ip http server
ip http secure-server
```

デバイス設定にどちらかのコマンドが含まれている場合は、HTTP サーバ機能が有効になっています。

前述のコマンドの出力に次の内容も含まれている場合

```
ip http active-session-modules none
ip http secure-active-session-modules none
```

このデバイスは、このアドバイザリに記載された脆弱性の影響を受けません。

脆弱性を含んでいないことが確認された製品

このアドバイザリの脆弱性のある製品セクションに記載されている製品のみが、これらの脆弱性の影響を受けることが分かっています。

シスコは、この脆弱性が Cisco IOS ソフトウェア、Cisco IOS XR ソフトウェア、および Cisco NX-OS ソフトウェアには影響を与えないことを確認しました。

詳細

Cisco IOS XE ソフトウェアの Web ベースのユーザ インターフェイス（Web UI）で複数の脆弱性が確認されました。認証された攻撃者が、昇格された権限を使用して、標的デバイスで任意のコマンドを実行する危険性があります。

これらの脆弱性は依存関係になく、 他方の脆弱性をエクスプロイトするために一方の脆弱性をエクスプロイトする必要がありません。 また、いずれかの脆弱性の影響を受けるリリースであっても、他の脆弱性の影響は受けない場合があります。

これらの脆弱性の詳細については、次のとおりです。

Cisco IOS XE ソフトウェアの Web UI で発見された、低い権限でのコマンド インジェクションの脆弱性

Cisco IOS XE ソフトウェアの Web ベースのユーザ インターフェイス（Web UI）で脆弱性が確認されました。認証されているが権限の低い攻撃者が、昇格された権限（レベル 15）を使用して、標的デバイスで Cisco IOS コマンドを実行する危険性があります。

この脆弱性は、標的対象のソフトウェアでユーザ入力が適切にサニタイズされないことに起因しています。 細工した入力パラメータを Web UI のフォームで指定し、そのフォームを送信することで、この脆弱性をエクスプロイトする危険性があります。 エクスプロイトに成功すると、攻撃者は権限レベル 15 のユーザとして任意の Cisco IOS コマンドを実行できるようになります。

この脆弱性のための Common Vulnerabilities and Exposures（CVE）ID は次のとおりです：
CVE-2019-12651

Cisco IOS XE ソフトウェアの Web UI で発見された、特権でのコマンド インジェクションの脆弱性

Cisco IOS XE ソフトウェアの Web ベースのユーザ インターフェイス（Web UI）で発見された脆弱性により、認証されたローカルの攻撃者が、影響を受けるデバイスの基盤となる Linux シェルで*ルート権限*を使用して任意のコマンドを実行できる危険性があります。

この脆弱性は、標的対象のソフトウェアでユーザ入力が適切にサニタイズされないことに起因しています。 標的デバイスの有効な管理者アクセス権（レベル 15）を持つ攻撃者が、細工した入力パラメータを Web UI のフォームで指定し、そのフォームを送信することで、この脆弱性をエクスプロイトする危険性があります。 エクスプロイトが成功すると、攻撃者が*ルート*権限を使用してデバイス上で任意のコマンドを実行し、それがシステム全体の侵害につながる危険性があります。

この脆弱性のための Common Vulnerabilities and Exposures（CVE）ID は次のとおりです：
CVE-2019-12650

回避策

これらの脆弱性に対処する回避策はありません。

HTTP サーバ機能を無効にすると、こうした脆弱性に対する攻撃ベクトルが排除されるため、対象デバイスのアップグレードが可能になるまでの適切な対応策となる可能性があります。 管理者は、グローバル コンフィギュレーション モードで **no ip http server** または **no ip http secure-Server** コマンドを使用して、HTTP サーバ機能を無効にすることができます。 HTTP サーバと HTTP セキュア サーバの両方が使用されている場合、HTTP サーバ機能を無効にするには両方のコマンドが必要です。

HTTP サーバへのアクセスを信頼できるネットワークのみに制限することで、これらの脆弱性のリスクが限定的になります。 次の例は、信頼できる 192.168.0.0/24 ネットワークから HTTP サーバへのリモートアクセスを許可する方法を示しています。

```
!
ip http access-class 75
ip http secure-server
!
access-list 75 permit 192.168.0.0 0.0.0.255
access-list 75 deny any
!
```

注: IOS XE ソフトウェアの新しいバージョンでアクセス リストを適用する場合、前述の例では **ip http access-class ipv4 75** コマンドを使用します。 『Cisco IOS デバイスの強化ガイド』には、デバイスを強化して管理アクセスのセキュリティを確保する方法が詳細に記載されています。

修正済みソフトウェア

シスコはこのアドバイザリに記載された脆弱性に対処する無償のソフトウェア アップデートを提供しています。 お客様がインストールしたりサポートを受けたりできるのは、ライセンスをご購入いただいたソフトウェア バージョンとフィーチャ セットに対してのみとなります。 そのようなソフトウェア アップグレードをインストール、ダウンロードする、または、アクセスしたり、その他の方法で使用する場合、お客様は以下のリンクに記載されたシスコのソフトウェア ライセンスの条項に従うことに同意したことになります。
https://www.cisco.com/c/en/us/products/end-user-license-agreement.html

また、お客様がソフトウェアをダウンロードできるのは、ソフトウェアの有効なライセンスをシスコから直接、あるいはシスコ認定リセラーやパートナーから取得している場合に限ります。 通常、これは以前購入したソフトウェアのメンテナンス アップグレードです。 無償のセキュリティ ソフトウェア アップデートによって、お客様に新しいソフトウェア ライセンス、追加ソフトウェア フィーチャ セット、またはメジャー リビジョン アップグレードに対する権限が付与されることはありません。

ソフトウェアのアップグレードを検討する際には、Cisco Security Advisories and Alerts ページで入手できるシスコ製品のアドバイザリを定期的に参照して、侵害を受ける可能性と完全なアップグレード ソリューションを確認してください。

いずれの場合も、アップグレードするデバイスに十分なメモリがあること、および現在のハードウェアとソフトウェアの構成は新規リリースでも継続して適切なサポートが受けられることを確認してください。 不明な点については、Cisco Technical Assistance Center（TAC）もしくは契約しているメンテナンス プロバイダーにお問い合わせください。

サービス契約をご利用でないお客様

シスコから直接購入したがシスコのサービス契約をご利用いただいていない場合、また、サードパーティ ベンダーから購入したが修正済みソフトウェアを購入先から入手できない場合は、Cisco TAC に連絡してアップグレードを入手してください。
https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

無償アップグレードの対象製品であることを証明していただくために、製品のシリアル番号と、本アドバイザリの URL をご用意ください。

Cisco IOS および IOS XE ソフトウェア

Cisco IOS ソフトウェアおよび IOS XE ソフトウェアの脆弱性による侵害の可能性を判断できるよう、シスコでは Cisco IOS Software Checker ツールを提供しています。このツールにより、特定のソフトウェア リリースに該当するシスコ セキュリティ アドバイザリ、および各アドバイザリで説明されている脆弱性が修正された最初のリリース（「First Fixed」）を特定できます。 また該当する場合、そのリリースに関するすべてのアドバイザリの脆弱性が修正された最初のリリース（「Combined First Fixed」）を特定できます。

このツールを使用して次のタスクを実行できます。

- ドロップダウン リストからリリース（複数可）を選択するか、分析対象となるローカル システムからファイルをアップロードして、検索を開始する
- **show version** コマンドの出力をツールで解析する
- カスタマイズした検索（過去に公開されたすべてのシスコ セキュリティ アドバイザリを検索対象に入れたり、特定のアドバイザリのみ、または最新のバンドル資料のすべてのアドバイザリを含めるなど）を作成する

リリースが、公開されたシスコ セキュリティ アドバイザリのいずれかに該当するかどうかを確認するには、Cisco.com の Cisco IOS Software Checker を使用するか、以下のフィールドに Cisco IOS ソフトウェアまたは Cisco IOS XE ソフトウェア リリース（たとえば、**15.1(4)M2**、**3.13.8S** など）を入力します。

デフォルトでは、Cisco IOS ソフトウェアのチェックには、結果は、高セキュリティへの影響の評価 (サー) または重大な脆弱性にのみが含まれています。 「中間」の SIR 脆弱性の結果を含めるには、Cisco.com の Cisco IOS ソフトウェア チェッカーを使用して、[Impact Rating] ドロップダウン リストの [中間（Medium）] チェックボックスをオンにします。

Cisco IOS XE ソフトウェア リリースと Cisco IOS ソフトウェア リリースのマッピングについて

は、Cisco IOS XE ソフトウェアのリリースに応じて「Cisco IOS XE 2 Release Notes」、「Cisco IOS XE 3S Release Notes」、または「Cisco IOS XE 3SG Release Notes」を参照してください。

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）では、本アドバイザリに記載されている脆弱性のエクスプロイト事例やその公表を確認していません。

出典

シスコは、この脆弱性（ID：CVE-2019-12651）の発見とご報告に関し、Verizon 社の Tahir Khan 氏のご協力に感謝いたします。 この脆弱性（ID：CVE-2019-12650）は、内部セキュリティ テストを実施中、ASIG（シスコの XB）によって発見されました。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190925-webui-cmd-injection

改訂履歴

バージョン	説明	セクション	ステータス	Date
1.2	IPSignature への追加されたリンク。	サイドバー	最終版	2019-October-11
1.1	CLI コマンドの出力内容を更新。	脆弱性のある製品	最終版	2019 年 9 月30日
1.0	初回公開リリース		最終版	2019 年 9 月 25 日

利用規約